INTERNATIONAL PREPAREDNESS

This section addresses what has been the most challenging aspect of the Committee's work this year—ascertaining the status of international Y2K preparedness.

BACKGROUND AND VULNERABILITIES

The days of American isolationism are long gone. An "American economy" is largely a misnomer—we now live in a global economy. The U.S. manufacturing sector imports commodities and components from a vast number of trading partners worldwide, and exports finished products to an equally vast number of customers worldwide. The software produced by the U.S. information technology sector is essential to businesses in every country in the management of their day-to-day operations.

Trade, which represents more than one-fifth of global output, is essential to the economic development and growth of all national economies.[1]No part of the U.S. economy is unaffected by international affairs, and significant Y2K-related disruptions suffered by any of our major trading partners have the potential to cause disruptions here at home.

Globalization is not limited to the economy, but extends to social and cultural issues as well. The technology that links us all has strengthened old friendships and created new ones in this increasingly small world. Significant Y2K-related disruptions suffered by our international friends and neighbors have the potential to raise the issue of humanitarian aid on an unparalleled level. Cries for such aid would inevitably be made to those nations most advanced in their Y2K preparations, including the U.S.

The scope of international Y2K preparedness is obviously a vast one. It has not been possible for any one organization to obtain definitive information concerning how our neighbors and trading partners around the world are progressing in their Y2K remediation efforts. A common problem faced by organizations making such efforts, including the Committee, is the uneven reliability of Y2K status information provided by nations themselves.

Indeed, there is an uneven global understanding of Y2K vulnerabilities, the unpredictability of cascading failures among interconnected systems, and the self-interest at all levels in either exaggerating or minimizing Y2K preparedness. Commercial firms marketing Y2K remediation services and governments soliciting external aid have an incentive To Whom It May Concern: overstate the Y2K problem. At the same time, fear of stimulating panic, sensitivity about disclosing security vulnerabilities, and concerns about legal liability are incentives to downplay the risks of Y2K failures.

In light of these informational shortcomings, the Committee is fortunate that multiple organizations, public and private, have undertaken the task of performing international Y2K assessments. The Committee's analysis of their combined findings reveals consistent results notwithstanding different approaches to the issue. As a result, the Committee believes that these findings, taken as a whole, provide a generally reliable indicator of Y2K status worldwide.

All of the vulnerabilities referenced in each sector of this report are present in every country around the world, to greater or lesser degrees. As the International Trade Administration concluded,

"Economies that are highly automated and in which computers, software, and networks are in widespread use have a greater chance of experiencing Y2K difficulties. At the same time, however, these economies also have greater access to the capital and human resources necessary to remediate systems and respond to Y2K-related needs. Countries that are less IT-dependent may have less Y2K exposure overall, but their essential services, such as power utilities and communications, may be highly computerized, while the resources to address potential problems may be in short supply."[2]

As discussed in further detail below, the Committee is particularly concerned about a handful of countries that are important to the U.S. for economic or strategic reasons. These nations include Russia, Japan, China, Italy, Venezuela, and Mexico.

One leading economic forecasting group, WEFA (formerly Wharton Econometric Forecasting Associates), identifies six risk factors for countries: hardware risk, aging capital stock risk, industrial structure risk, import supply chain risk, export financing risk and infrastructure risk. Ultimately, the riskiest countries are those with high vulnerability according to the risk factors and low spending (effort) for fixing Y2K problems.

WHAT IS BEING DONE?

Numerous entities, public and private, have spent much of 1999 conducting regular assessments of the Y2K preparedness status of countries around the world. The following section summarizes the work done by a few of these organizations.

U.S. State Department

The U.S. State Department (DOS) has been monitoring the status of international Y2K preparedness efforts for several reasons, chief among them the desire to avoid potential difficulties that might face U.S. embassies and foreign posts on January 1, 2000. DOS has conducted ongoing surveys among its 260 posts around the world to ascertain and monitor the Y2K status of host countries.

DOS earlier issued an edict stating that all embassies must be prepared to be self-sufficient for 30 days by January 1, 2000. DOS has established early October as the time by which it will make decisions as to whether it is appropriate to draw down personnel at any of these international posts for Y2K reasons.

DOS's other principal interest in monitoring international Y2K preparations is to ensure the safety of Americans abroad. In this regard, on September 14 DOS posted biannual consular advisory for 172 nations which included, for the first time, Y2K-related information. These consular advisories are posted at http://travel.state.gov. The Y2K-related language in this initial wave of advisories is rather general, with little to distinguish one country from another.

In contrast, DOS's Office of the Inspector General (OIG), which is engaged in Y2K assessments of numerous countries, has provided valuable testimony to the Committee in two hearings this year, most recently in a July 22 hearing on global corporations. At that time, the OIG had assessed 161 countries, with the following summary results:

- About half of the 161 countries assessed were at medium to high risk of having Y2K-related failures in their telecommunications, energy, and/or transportation sectors.

- Industrialized countries were generally at low risk of having Y2K-related infrastructure failures, particularly in the finance sector. Still, nearly a third of these countries (11 of 39) were at medium risk of failure in the transportation sector, and almost one-fourth (9 of 39) were at a medium or high risk of failure in the telecommunications, energy, or water sectors.

- Between 52-68 developing countries of 98 had a medium or high risk of Y2K-related failure in the telecommunications, transportation, and/or energy sectors. However, the relatively low level of computerization in key sectors of the developing world may reduce the risk of prolonged infrastructure failures.

- Key sectors in the newly independent states and the other former eastern bloc nations are a concern because of the relatively high probability of Y2K-related failures.

U.S. Agency for International Development (USAID)

USAID has made a tremendous contribution to our understanding of the potential impact of Y2K in developing countries. For many in the Administration, Y2K problems in developing nations are shrugged off with comments that "Country X" has problems with electric power on a good day; why would Y2K be any worse. This oversimplification demonstrates the lack of an understanding of margins, i.e. the difference between having a failure and having the technical and financial resources to fix the failure.

Developing nations are more vulnerable to Y2K failures not because they are as reliant on IT as industrialized nations, but because they have smaller margins. For example, failures and disruptions in key systems such as those used to control electric power or to deliver pension checks becomes longer lasting and, thus, more serious if the country does not have the resources to detect and fix the problem.

According to the Institute of Electrical and Electronics Engineers (IEEE), *"Y2K is a long-term, not a short-term problem . . . Y2K computer problems will be causing computer systems malfunctions and failures into the next decade*." This may be especially true in developing nations where the expertise to fix such systems is not readily available. Further, developing nations are often unable to compete with developed nations in buying "rapid" IT solutions.

USAID has also begun an effort to assemble a Global Y2K Consortium. This consortium would bring technology expertise from U.S. global corporations to bear in the respective countries where they operate.

United Nations

In June 1999 the United Nations (UN) hosted a meeting of national Y2K coordinators in New York City. The national Y2K coordinators from more than 170 countries met to discuss Y2K preparations and exchange information.

There was an attempt to gather an international assessment of key sectors. However, the uneven understanding of technology and key country sectors impeded the attempt to build a reliable assessment. There was a great deal of discussion of "publicizing" Y2K and the appropriate public relations. There was notable progress in trying to address the transborder issues that could result from individual countries exercising contingency plans. Unfortunately, many countries appointed Y2K coordinators with little political power. So it was difficult to assess the success of these discussions.

There was also a significant difference between the public and private conversations that were taking place between country coordinators—the public picture of Y2K readiness always rosier than the private one. The end result of the conference was that the world knows more about what is happening, but not enough to obtain a clear picture of the worldwide Y2K situation.

The UN could greatly facilitate the speed and efficiency with which world problems resulting from Y2K are resolved. However, the UN needs to first take care of its own Y2K readiness as an organizational body. Currently, there is no a clear understanding of its internal readiness or that of its agencies.

The IY2KCC

On August 26, 1999, the International Y2K Cooperation Center (IY2KCC), a UN-backed group

funded by the World Bank, released its first survey of Y2K readiness in 72 nations, as reported by national Y2K coordinators representing each government. The survey asked these national Y2K coordinators to report the month implementation was expected to be 90% complete for various sectors. Full survey results can be found at the IY2KCC's web site, at www.iy2kcc.org. While the survey will be continually updated, as initially reported it yielded only 72 responses—67 countries had not yet responded. The following are a few summary findings:

- The health sector reported the latest completion dates, followed by the government services sector. The finance sector reported the earliest completion dates.

- Eastern Europe/Central Asia and South America, with 40% and 70% of countries reporting respectively, reported the latest average completion dates.

- Sub-Saharan Africa reported the least dependence on technology in its critical sectors, followed by Eastern Europe/Central Asia, Central America/Caribbean, and the Middle East/North Africa. North America and Western Europe reported the highest dependency on technology.

- Eleven countries (15%) had completed their healthcare contingency plans; twelve countries (17%) had completed their government services contingency plans; and 28 countries (39%) had completed their energy contingency plans.

More specifically, the U.S. and several other countries reported that certain sectors would not be ready until the last weeks of 1999. December targets were set by the U.S. for healthcare; by Pakistan and Macedonia for air transportation; by Bulgaria for healthcare; by Bolivia for government services; by Colombia for customs; and by Angola for sea and land transportation, customs, and healthcare. Bolivia also would not be ready with its customs system until after 1999, and Slovakia does not expect to complete remediation of its healthcare system until after the new year.

European Commission

In December 1998, the European Commission (EC) adopted a report, "How the EU is tackling the Year 2000 Computer Problem," which was presented to the European Council. The Council asked the EC to convene a meeting of representatives of public infrastructure providers from the member states to establish if cross-border dependencies in such areas as transport, energy, and water supply were being adequately addressed.

In April 1999, the EC hosted a two-day meeting of EU public infrastructure providers. On June 2, the EC issued a report on the preparedness of key EU infrastructures for the Y2K problem.[3] While steady progress was reported overall within the EU, there were indications that not all sectors in all member states ex-

pected to be totally ready and fully compliant in time. A major problem was the lack of available verifiable information on the situation, particularly in relation to the potential spillover effects between member states.

In addition, every sector reported that smaller organizations lagged significantly behind larger companies in addressing the Y2K problem, and all organizations were dependent upon their information technology systems suppliers to accurately disclose Y2K compliance and deliver timely compliant upgrades.

With regard to the situation beyond the EU's external borders, the assessment of possible safety issues in nuclear installations and power grids in Eastern Europe and the former Soviet Union was of perhaps the most concern.

The findings with respect to some of the specific sectors were as follows:

Electricity: There may be failures, likely to be localized, which in the middle of winter could have serious consequences for the areas concerned.

Gas: The cross-border effect for natural gas was significant, since 43% of natural gas originates from outside the EU. Moreover, 22% of the total energy demand is covered by gas. These external supplies are obtained primarily from Russia, Algeria, and Norway, and the gas must flow across several countries through major pipelines to reach the various destinations. The report concluded that contingency plans were essential to assure uninterrupted and safe gas delivery.

Oil: Substantial oil stocks should exist, but the dependence on non-EU oil supplies, at nearly 80%, is high, and it is not possible to be certain of the effect of Y2K on external producer countries.

Nuclear safety: Member states of the EU have action plans to address the issue, and most reactor operators report they will be Y2K ready by mid-1999. As for outside the EU—the Central and Eastern European countries and the Newly Independent States--there is a lack of confidence that concerns have been appropriately checked, including contingency plans. No guarantees can be given that assessments will be performed in time or that contingency plans will be ready. No international organization is presently able to coordinate an assessment of the risk presented by grid failure in these countries. In view of the potential risk to nuclear power plants; to imports from the Newly Independent States such as gas; and the general risk to citizens in the these countries, urgent attention needs to be paid to this issue.

Water supply and wastewater treatment: The main risk identified is the possibility of pollution of surface waters used for drinking water abstraction intake from major rivers as a consequence of the Y2K problem.

Telecommunications: The strong possibilities of network saturation give rise to the clear need to en-

sure a continuing priority to emergency and other essential services. It is considered that operators outside the EU may not be equally well prepared and that disruption to the international telephone and fax networks cannot be excluded.

Healthcare: No international body is addressing the sector and no exchange of information is taking place between countries. The main problem is the difficulty in obtaining information from suppliers on the compliance of products, especially electronic machines for medical and health purposes containing embedded chips, in use within hospitals.

Global 2000 Coordinating Committee

Global 2000, an informal organization of banks, securities firms, and insurance companies, is a voluntary, private-sector financial industry grouping made up of 630 institutions from 70 countries. Its creation was announced at the Bank for International Settlements' Year 2000 Roundtable, which established the Joint Year 2000 Council in Switzerland in April 1998. Global 2000's mission is to identify and resource areas where coordinated initiatives will facilitate efforts by the global financial community to minimize the risks to global financial markets arising from the Y2K problem.

International Monitoring

International Monitoring (IM) is a London-based specialist consultancy that provides information assessing the potential scale of Y2K damages and delays to 140 countries. It issues a Risk Rating report covering Africa, the Americas, Asia & Pacific, Europe, and the Middle East. To arrive at its risk ratings, the firm inventories country technology resources and utilization profiles to chart assessment progress; projects bad and incomplete fixes; and assesses economic profiles, technology usage and import-expert dependencies. The estimate of Y2K damage ranges from 0.0 to 9.0 and assesses scenarios in terms of delay or degradations in various sectors.

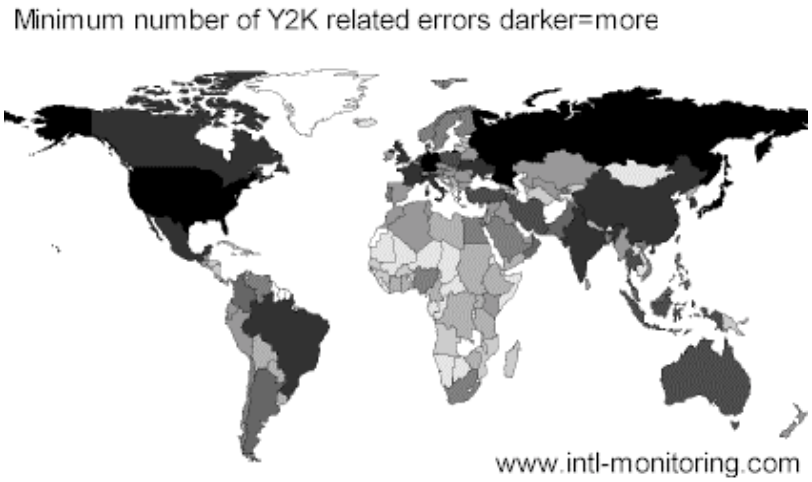

Figure 1 – Y2K Status of Countries of the World

On August 26, IM released its assessment of projected Y2K-related security risk exposure worldwide. Figure 1, available on IM's web

site, depicts the country by country assessments contained in the report. The report measured the risk to foreign entities and individuals of being in given nations around the century date change. Counties listed as posing extreme risk were Albania, Bangladesh, Colombia, Congo, Zaire, Egypt, El Salvador, Ethiopia, Guinea, Guinea-Bissau, Haiti, Indonesia, Kenya, Lebanon, Liberia, Madagascar, Moldova, Myanmar, Niger, Nigeria, Pakistan, Qatar, Russia, Somalia, Sudan, Turkey, Vietnam, and Yugoslavia.[4]

IM's August 20 update showed the average country slightly lowering its Y2K risk. One of the most improved countries was Mexico. However, 21 countries slipped further behind in their efforts and the vast majority of are countries still showing significant risk of infrastructure failure. The most disappointing country was Russia. Taiwan and Malaysia are also considered to be increasing their risk by falling behind in already late Y2K projects. The best gains are being made in the financial services sector, while transportation was falling behind in 27 of the 49 countries. IM believes that a failure in transportation could raise significant issues for supply chains.

IM's scenario for most countries still indicates significant potential for infrastructure failure possibly lasting anywhere from 2 days to 8 weeks.

Global Corporations

Committee staff discussions with numerous global corporations show that all major global corporations are engaged in detailed international Y2K assessments for internal use. These firms have a huge stake in ensuring their continued business operations in their factories and sites abroad, and are taking proactive measures where possible and defensive measures where necessary.

While the assessments of these corporations are generally proprietary and, therefore, not for public use, several global corporations have stepped forward to share their general assessments. For example, during the Committee's July 22 global corporations hearing, Philip Morris—with 220 factories in 50 countries and business in more than 180 different markets—testified that it then considered approximately 600 of its highly critical international business partners to be likely to suffer Y2K related failures. As a result, Philip Morris believed it would suffer disruptions in its supply chain due to Y2K failures at these facilities, and

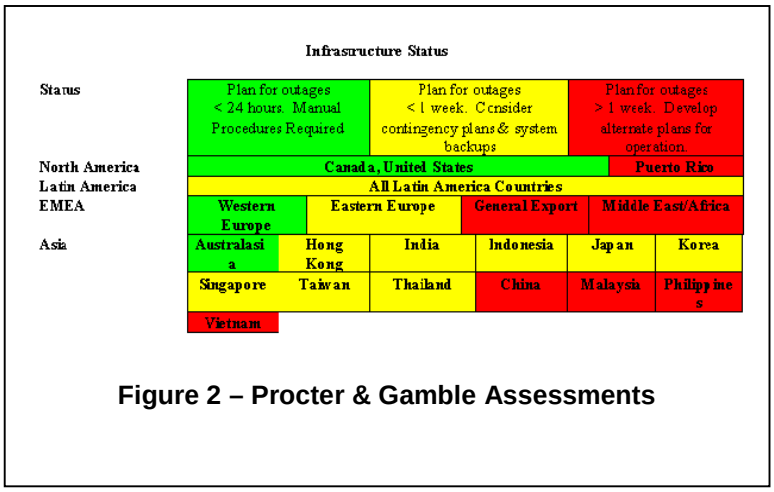

Figure 2 – Procter & Gamble Assessments

was taking steps to minimize the effects of these disruptions.

Another witness at that hearing was Procter & Gamble, which testified about its detailed international assessments, including international utility risk assessments. Its results are depicted in figure 2.

STATUS

Top-Tier Countries

Every assessment known to the Committee indicates that Canada, Australia, and the United Kingdom are at the top of the Y2K preparedness lists.

Canada: As of August 26, the Canadian government reported that 99% of its mission-critical systems were Y2K compliant. A February-March 1999 survey on Canadian industry, published in June, showed:

- 52% of large corporations expected to have all of their critical systems ready before the end of June; this was expected to increase to 85% by the end of September.

- About 87% of small organizations and 98% of medium organizations with critical systems had taken at least some steps to ensure these systems would function when the date changes to the Year 2000.

- Despite this progress, there was still substantial work to be done. At the time of the survey, only 15% of all large organizations with plans to test critical systems said testing had been completed. An estimated 13% said testing had not even started, and an additional 9% said testing had started but was less than halfway to completion. There was also evidence that the work done to date was not progressing as quickly as expected.

- In most sectors, at least 75% of large organizations said they would complete all Y2K preparations required to ensure the continued delivery of products and services before the end of September. The only exception was the health sector, where 49% of large hospitals and 33% of large care homes said they would not complete their preparations until sometime during the last quarter of 1999.

- Among large municipalities, 34% of police, 9% of ambulance, 22% of fire, 17% of water and 17% of sewage services said they would not finish critical preparations until after September.

A poll undertaken by the Canadian Federation of Independent Business, with results published in September 1999, showed that 92% of firms that employ fewer than 50 people say they are ready to handle the Y2K transition. However, only 77% of these firms had contingency plans.

Australia: Australia has created a Year 2000 National Strategy and established public and private sector task forces. In addition to con-

fronting the Y2K problems faced by the commonwealth and states, Australia has established a National Industry Steering Committee (NSC), whose task is to develop and implement a $10 million Industry Program to increase business awareness of the Y2K problem.

As a followup to an October 1998 survey, an Australian Bureau of Statistics survey was commissioned by the NSC in 1999, with preliminary results issued on August 31.[5] The survey shows that

- More than one-third of all businesses reported they had completed their Y2K work; more than three times the number of businesses which had reached this stage by the end of October 1998.

- The proportion of businesses not intending to undertake any Y2K work has remained constant at 40%. Typically these are small businesses with less than 5 employees and low levels of technology dependence. Almost two-thirds of the businesses not intending to undertake any Y2K work reported that their only technology was communications equipment or a stand-alone computer. The majority of businesses that do not intend to undertake any Y2K work reported that they either don't have any technology that will be affected or they don't believe their business will be affected.

- Of the businesses intending to undertake Y2K work, nearly all had started work by the end of June 1999. Virtually all businesses that hadn't already completed their Y2K work expect to be completed by December 1999.

Australian business expects to spend approximately $10 billion addressing the Y2K problem.

United Kingdom: The United Kingdom's most recent status report on the national infrastructure was released on July 13, 1999, with status given as of May 14. Sectors were rated red for severe risk of material disruption, there may not be enough time to rectify; yellow for some risk of material disruption but agreed rectification and containment plans are in place; and blue for assessment has not identified any risk of material disruption. Some preliminary red and yellow results and percentages of the sector that color are:

<u>Red</u>

- Local government: 1% red for England and Wales and 12% red for Scotland.

<u>Yellow</u>

- Electricity: 5% yellow
- Mains gas: 10% was yellow for domestic shippers and suppliers
- Oil fuels: 18% was yellow for the supply of heating and transport fuel
- Food and Groceries: 9% yellow
- Airlines: 13% yellow
- British business and operational systems: 30% yellow
- London Underground: 25% yel-

low
- Buses: 25% yellow
- Ports: 15% yellow
- Shipping: 45% yellow
- Police forces: 98% yellow
- Fire brigades: 41% yellow
- Healthcare: 97% yellow
- Tax collection: 62% yellow

Western Europe

Since the Committee's prior report, Western Europe has become increasingly aware of critical sector interdependencies existing within telecommunications, energy, water, transportation and finance. This increasing awareness has brought about extensive progress towards Y2K remediation and preparedness. News from the EC had reported that Y2K concerns lagged behind the efforts toward the currency changeover to the euro. However, more recent reports indicate that the euro conversion has been profitable for Y2K remediation because industries and government agencies were already in the process of updating systems to handle the euro. Businesses find it advantageous to complete Y2K assessments and remediation at the same time.

As a general matter, throughout Western Europe the financial sector is the most advanced critical infrastructure in remediation. However, the financial sector is dependent on both the energy and telecommunications sectors, which tend to trail behind in addressing the Y2K problem. Further, small European businesses are significantly behind large industries and companies attending to Y2K issues.

Germany: According to a German Federal government report released in April 1999, Germany is quite advanced in its preparation for the Year 2000. A 1999 government survey of the 30 largest power supply firms and 37 smaller utilities groups showed that all companies had projects and contingency plans underway, although some were further along than others.

The financial sector is particularly well prepared and the telecommunications sector has made intensive efforts towards remediation. All three sectors announced that no noticeable fallouts had been expected. However, healthcare poses serious risks, and small- and medium-sized businesses are lagging significantly behind larger corporations. Small- and medium-sized firms started their Y2K work relatively late compared to large firms, but are under considerable pressure to become compliant. The German government is actively involved in providing advice and information to potentially affected firms, specifically small- and medium-sized businesses.

Italy: Italy started Y2K preparedness initiatives considerably later than other western European countries. The Comitato Anno 2000, a joint public/private sector Y2K coordinating body, was not established until December 1998, and met for the first time in January 1999. At a June conference in Rome, Ernesto Bettinelli, the Committee Chair, stated, ". . . *only two days ago I received*

the findings of a fresh survey conducted . . . on the level of awareness of the Italians on the Millennium Bug problem: only 15% of the respondents [are] aware of the problem with less than half of the year left to December 31, 1999. It could even be taken as a good news: Ignorance and Disinformation: the Italians show the way to avoid mass panic so feared abroad."[6]

Specific areas of concern are water, electric utilities, transportation, airports and, appearing weakest, adaptation of hospital equipment. Also disquieting is the fact that hundreds of thousands of people from around the world are expected to converge on Rome at the end of the year to commemorate what they believe to be the 2,000th anniversary of the birth of Christ.

France, Spain, Portugal: Reports on France indicate that most government agencies began their Y2K work several years ago. The Gartner Group world status report suggests that, overall, France ranges from having at least 20% of remediation completed, plans are in place, and resources committed to being fully compliant. Energy, gas, and electricity industries are mostly through completion and have contingency plans in place. Both Spain and Portugal also range from assessing Y2K status in all sectors to becoming fully compliant.

Austria, Belgium, Switzerland: Austria, Belgium, and Switzerland generally appear to be in the final stages of remediation of mission-critical sectors. Belgacom, a large Belgian telecommunications provider, stated in May that "all planned inventories, analyzes and assessment have been finalized and trial runs completed."[7] Switzerland disclosed that there are no indications of large-scale risks. Although they cannot be sure of any shortcomings, because of the extensive work done in all key areas, risks should be quite limited. In May, Switzerland announced: "The reliability of services and the operating capability of the public and private sector are at risk of disruption today and every day. There are precautionary measures (contingency planning) in place, designed to offer protection against the effects of such disturbance. They are part of normal business and everyday planning."[8]

Denmark, Finland, Iceland, Netherlands, Norway, Sweden: The Gartner Group Year 2000 world status report for the second quarter of 1999 categorizes all of these countries to be steadily underway on becoming Y2K compliant. Plans tackling the problem are complete and resources have been allocated. Each country ranges from having at least 20% of remediation completed to being fully compliant in each mission-critical area. Nearly all of the key sectors tend to be highly dependent on technology in each nation, implementation plans have all been scheduled to be completed by October. Norway, Sweden, Iceland, Denmark, and Finland have the highest reliance on information and communications technology, energy, and trade exposure in most of western Europe. However, they appear to be the most prepared.

Greece: Greece could possibly face serious technical problems in all of the following sectors: healthcare, water, transportation, public service, communications, and energy. The financial sector is at low risk.

Eastern Europe

All available assessments indicate that, as a general matter, key sectors in the countries that were part of the eastern bloc, including those that were part of the former Soviet Union, have a relatively high probability of Y2K-related failures. Most at risk are fails in the telecommunications, transportation, and energy sectors.

As noted above, the EU has serious concerns regarding the nuclear safety of plants located in this region.

Russia: Russia is the 30th largest U.S. trading partner and hosts 11,000 U.S. citizens. While it is neither the largest trading partner nor the biggest host of expatriate citizens, Russia is of major importance to the U.S. Russian economic and military stability are key concerns for the international community. The cost of fixing Russian's Y2K problems was projected to cost anywhere between $1.5 and $3 billion, which could equal 1.8% to 2.7% of Russian Gross Domestic Product. Finally, in July, Finance Minister Mikhail Kasyanov stated that $187 billion would allow Russia to fix its problems. He noted that the government would prioritize funds for defense and security.[9] In July 1999, Russia projected that government readiness was at about 35%, with the readiness of the energy sector somewhere around 50%.

Aside from government readiness, Russia faces major Y2K challenges in key infrastructure sectors including telecommunications, energy, banking, and government services. In June of 1999 it was projected that Russia was likely to experience a month of disruptions in financial markets, two months for utilities and healthcare, and up to three months of turmoil in transportation and telecommunications.

Disruptions in key sectors such as telecommunications could be a significant impediment to Russia's economic recovery, as well as its ability to confront Y2K situations as they arise. There is an inconsistency in the approach and implementation of Y2K fixes in Russian telecommunications. In some cases, money is clearly the problem. In other cases, concerns over national security have prompted carriers not to discuss or share readiness concerns and remediation plans. A major long distance carrier in Russia is reportedly opting to create "work arounds" for its seven gateway switches instead off replacing them.

In the new global economy, where organizations strive to be transparent and responsive to market changes, Y2K has provided an unexpected benefit. Y2K has enable many complex organizations to get control of their IT infrastructures and stream line core process and functions. Unfortunately, in many cases, *"Russia will only get yet another set of "workarounds" that prolong*

the life of already obsolete systems. On the surface the result will be the same–no particularly huge catastrophes…but the Western method may create more wealth … while the Russian method may diminish it."[10]

On September 13, DOD and the Russian Ministry of Defense (MOD) signed an agreement for the U.S. and the Russian Federation indicating their intent to establish the Center for Year 2000 Strategic Stability (CY2KSS) during the Year 2000 transition period. Secretary of Defense William S. Cohen and Russian Federation Minister of Defense Igor Sergeyev formally signed the statement in Moscow today.

In the CY2KSS, U.S. and Russian military personnel will sit side-by-side during the Y2K transition period, from late December 1999 to mid-January 2000, and continuously monitor U.S.-provided information on missile and space launches. These people will be in voice contact with command centers in the U.S. and Russia via a highly reliable, Y2K-tested communications link.

In addition to missile and space launches, the center will serve as a means to communicate about other defense-related events that could be potentially destabilizing, such as an aircraft going off course due to a Y2K failure of a navigation or communication system.

The CY2KSS complements the extensive steps taken by both the U.S. and Russia to ensure the Y2K reliability of their warning systems, nuclear weapons, and command and control capabilities. Both countries agree that the likelihood of Y2K failure in these systems is extremely remote and that sufficient safeguards are in place to handle these situations. However, given the potentially severe consequences, the establishment of the center is a worthwhile investment.

Discussions on the CY2KSS began in February 1999. Peterson Air Force Base in Colorado Springs, Colorado, was chosen as the center's site because of its accessibility to U.S. information and the desire to use the facility after the Y2K transition to train U.S. personnel for duty in a permanent Joint Warning Center to be established in Moscow. The total cost of the establishment and operation of the CY2KSS is approximately $8 million. The center is currently on schedule to be completed on Dec. 1, 1999. The CY2KSS is one component of a comprehensive DOD-related Y2K cooperation program that began to take shape in February 1999. In addition to establishing the CY2KSS, the U.S. and Russia have four other efforts:

- exchanging Y2K experiences to help each other manage the Y2K problem and to understand each other's management plans and progress;
- ensuring the direct communication links between our national leaders remain reliable;
- maintaining the security of the Russian nuclear weapons stockpile;

- exchanging Y2K experiences related to nuclear forces to maintain reliable nuclear command and control.

Defense issues are only one part of the equation. Oblasts, krays, republics, and okrugs comprise the 88 administrative regions of the Russian Federation. Each region has its own unique set of Y2K problems. The rhetoric about individual responsibility for addressing the Y2K problem has been plentiful, but funds have been scarce.

Successful information exchanges continue to take place between DOE and the Russian Federation. In October 1998, DOE held its first Y2K workshop in Moscow. In January 1999, DOE published Y2K guidance with the International Energy Agency (IEA). DOE also held a workshop for transmissions and distribution systems in February. In spring of 1999, DOE collaborated with the International Science and Technology Center in Moscow and funded 11 Y2K projects, the majority of which were nuclear-specific. On September 9, a delegation of Russian and Ukrainian experts came to the U.S. to observe the NERC electric power drill. Further, the IEA is planning a contingency conference in Prague in October.

Nuclear power plants have been a serious concern for Russia. Russia has 29 nuclear power reactor units in operation at nine sites, producing a total of approximately 21,000 MW per year. In 1997, the nuclear power plants in Russia produced 14% of the electricity; in the far Western parts of Russia, the share was 24.9%. The Leningrad (Sosnovyy Bor), Kola, and Smolensk nuclear plants supply half of northwest Russia's electricity requirements. In addition to nuclear power, Russia generates about 70% of its electricity at thermal power stations (coal, gas, and oil) and about 18% at hydroelectric stations.

Western-style plants employ the design principle of safety in depth, relying on a series of physical barriers--including a massive reinforced concrete structure called the containment--to prevent the release of radioactive material to the environment. With the exception of some VVER designs, Soviet-designed reactors do not have such a containment structure. Soviet-designed reactors are essentially variations on two basic designs: the VVER--or pressurized light water--type, and the RBMK--the graphite moderated, channel reactor. Three generations of Soviet-designed VVER reactors--upgraded over time--are operating in Eastern Europe and the former Soviet Union.[11] *RBMK reactors are more commonly known as the Chernobyl style plant. About 97 percent of Russia's nuclear generating capacity comes from reactors built to the RBMK and VVER designs.*[12]

According to DOE, U.S.-Russian collaboration has helped improve safety in the Soviet-era plants and reduced the number of operational events from 128 in 1994, to 95 in 1995. Of the 1995 incidents, 57 occurred at VVER units and 38 at

RBMK and other units. Unplanned disconnections from the grid were greater at VVER units than at other units.[13]

Russia and DOE have found no Y2K issues in primary plant safety systems. Primary plant safety systems monitor specific plant parameters (temperature, pressure, level, flow, reactor power) and provide automatic control and protection actions for plant safety. Primary plant systems can be thought of as the front line defense against accidents. There are also systems that are important to safety and have an indirect impact on plant operations. These are systems used to monitor (not control) plant functions such as steam generator level, synchronize plant clock. The most critical piece of equipment which will face Y2K challenges is the plant process computer and its related information display and data archiving systems. If these fail or experience problems, they will not cause an accident. However, the malfunction of these systems would complicate operations and increase the opportunity of operator error. The combination of human error and computer error is a challenge not just for the Russians but the entire world.

Ukraine: Ukraine faces many challenges in addressing Y2K; it has been difficult for this emerging nation to focus and fund its Y2K efforts. The good news is that Ukraine has enjoyed strong support from it senior leadership including the President. Unfortunately, the Ukraine lacks the resources of the Russian government in addressing its problems.

Ukraine faces many of the same challenges that Russia does and co-ordination between the two nations will be key.

The Ukraine relies on nuclear power for 46% of it electric power and must address the same nuclear power plant challenges as Russia. The U.K. reports that loss of power output is possible and could cause significant disruption to the electricity grid. Russian natural gas and oil pipelines could be compromised by such breakdowns in electric power. Electric power distribution managers in Ukraine have been working closely with the U.S. to develop contingency plans and prepare for possible disruptions.

Asia

International Monitoring estimated on July 2 that the ASEAN countries—which include Malaysia, the Philippines, Singapore, Thailand, and Vietnam—would suffer Y2K-related delays and damages totaling more than $90 billion combined.[14]

China: China has economic importance to the U.S. China is the 4th leading exporter and the 12th leading importer to the U.S. The U.S. has over $5 billion in investment in China. Because of improper planning, insufficient resources, and a very late start in addressing the Y2K problem, the Committee believes that a substantial portion of Chinese companies and the government will experience several failures in their computers.

China's relatively low dependence on computers, particularly in the rural areas in many provinces, is in this case a benefit from a Y2K standpoint. However, it is technology dependent in its major cities and highly commercial provinces. Experts predict serious infrastructure failures in these areas.

Of particular concern to the Committee is that many of China's electric power plants are Y2K vulnerable and there is little evidence that China is remediating systems. Plants are difficult to run manually and blackouts could result. Electric power outages could impact other sector services such as telecommunications, and oil and gas.

Exacerbating China's Y2K problems is the fact that 80% to 95% of its software is thought to be pirated. This could prevent Chinese companies from receiving technical support from suppliers. Despite this assertion, some believe that cash-strapped Chinese companies may elect to sue American suppliers for failures and losses instead of concentrating on remediation. If true, this is very troubling to the Committee.

Japan: Next to the United States, Japan has the greater dependence on technology than any other country of the world. It is for this reason, Japan's late start in addressing the Y2K problem, and its importance as a trading partner to the U.S., that the Committee remains concerned about Japan's Y2K preparedness.

While Japan has made tremendous strides over the past six months to catch up, the amount of Y2K work it has to do puts it well behind the U.S. in addressing the Y2K problem. It did not prepare a national action plan until September 11, 1998—nearly one year behind most other highly industrialized nations. Since that time, it has been mirroring the U.S. and Great Britain in its approach to the problem.

According to Japan's self reported information as of July 1999:

- about 72% of the financial sector (banks, insurance, and securities) have completed testing of their systems.
- 98% of the electric and oil sectors had completed testing of their systems.
- 91% of the critical control systems in the oil industry had completed testing.
- 69% of the telecommunications networks had competed testing.
- 97% of their critical aviation systems had been tested.

Of most concern is the healthcare sector, and small and medium sized enterprises. The later could have a significant impact on Japanese enterprises, and thus U.S. enterprises. The heart of the Committee's concern is that with just 100 days to go before the date rollover, simply has too much to do. Its catch up status makes it prone to errors during remediation, and thus more ex-

posed to undetected Y2K problems.

The Philippines: The Y2K Commission has a mandate to closely monitor the nation's Y2K compliance. As part of that mandate, it conducts a regular monthly survey of firms and organizations in mission-critical sectors. The most recent survey, from August 1999, showed the following rates of overall compliance: telecommunications and utilities and at 77%; transportation at 76%; finance at 93%; healthcare at 69%; manufacturing at 71%; and government services at 75%.

The government has set a September 30 deadline for all firms and government agencies to become Y2K ready. By that time, the government plans to release a list of thousands of companies and agencies that have failed to document their Y2K readiness. So far, fewer than 1,000 of 18,000 companies required to be Y2K compliant have disclosed their level of Y2K readiness. In October the Commission will conduct a validation of compliance reports submitted by companies and government agencies to determine their veracity.

Thailand: In April 1998, the Thai cabinet appointed a National Y2K Coordination Committee and a national plan was set up to solve the Y2K problem in four "super-critical organizations"—power and energy; financial, banking, and insurance; telecommunications and transportation; and social order. The status of these sectors as of July 26 was as follows:

- All entities in the power and energy sector were reported to be 100% compliant;
- Most entities in the finance, banking, and insurance sector were 100% compliant except the Revenue Department (88%), the Department of Insurance (42%), and the Government Lottery Office (55%);
- Almost all entities in the telecommunications and transportation sector were 100% compliant except the Meteorological Department (67%) and the Ministry of Transport and Communications (86%); and
- As far as the social order sector, the Ministry of Defense is 80% compliant and the Bangkok Metropolitan Administration is 68% compliant.

On August 14, the Deputy Prime Minister told the Thai cabinet that 65% of the 231 government agencies that use computers in their main tasks have reported they had fixed them. These included most of the government agencies that were a top priority. However, the Deputy Prime Minister also said the remaining 35% had made little progress. The overall situation in the country was still considered "worrying."[15]

Vietnam: Vietnam has established a Y2K Steering Committee and issued the following August 22, 1999 report. Eighty percent of central organizations; 59% of provinces and cities; and 86% of corporations had undertaken corrective measures.

However, more than 50% of small- and medium-sized enterprises are not aware of Y2K at an adequate level and have not taken necessary actions.

As of August 25, 94.73% of central and local organizations and enterprises had made an inventory and assessment of the impact of Y2K, with the following results:

- Of the 108,147 computers checked, 50,146 were not Y2K compliant. That amounts to 46% of the total PCs in public administration and state enterprises. Of these, .85% are used for very important applications, and 25.35% are used for important applications.

- About 70% of systems software was not compliant, of which 50% could be repaired by upgraded software. The malfunctioning of 1% of this software would have a very serious impact, and the malfunctioning of 35% would have a serious impact.
- About 90% of applications software was not Y2K compliant or its status was unknown. The malfunctioning of 76% of this software would have a very serious impact (mainly applications in financial, banking, postal, and airlines functions) and the malfunctioning of 8% would have a serious impact.

- Of 8,394 pieces of equipment with embedded chips checked, 4,183 were not compliant—49.83%. The malfunctioning of 1% of these chips would have a very serious impact, and the malfunctioning of 71% of these chips would have a serious impact. However, embedded systems have not been completely checked and assessed.

The progress of the financial branch is slower than others and Vietnam reports that, in the next months, special measures should be taken to overcome the problems in time. The electricity and health branches have many difficulties in addressing the problem for automated control equipment and specified health equipment with respect to embedded chips. Other non-key ministries, organizations equivalent to a ministry, provinces, and cities are making very slow progress. Vietnam reports that if there are no special measures, the problem will not be solved in time and there will be a considerable impact on state management, business, and production activities.

Korea: The Prime Minister's office established a Year 2000 Conversion Council in April 1998 to check the progress, in each area, to detect problems, and to discuss aids. The Ministry of Information and Communication established The Year 2000 Task Force and has acted to oversee mission critical sectors. The Task Force implemented the government's Y2K Action Plan.

The status report by the end of July 1999 was as follows:

Banking and Finance 99.9%
Electricity and Energy 99.8%
Nuclear Power Plants 100%
Transportation 99.8%

Industrial activities 98.6%
Defense 97.7%
Telecommunications 97.3%
Water Resources 97.8%
Central and Local Government 96.7%
Health 95.9%
Environment 100%
Shipping/Ports 100%
Small and Medium Business 90.2%

The central and local government, and the small and medium business sectors, are behind Korea's established schedules.

During 1998, 4.37 billion won was used as the Y2K budget, and 17.38 billion won is allocated for 1999.

In 1999 the government is providing field inspections for 10,000 SMBs and experts and funds for 2,000 SMBs. The progress of 500 selected SMBs is monitored monthly. In addition, SMBs are fixing the Y2K problem in conjunction with large companies. 61 large cooperative groups are expected to help their affiliate SMBs Y2K readiness by September.

Latin America

Dramatic progress has been made in recent months in Latin America, which includes, for purposes of this report, the countries of Mexico, Central America, and South America. Early attention on the large emerging-market of Brazil has translated into substantial progress over the past year. However, many countries in the region continue to play "catch-up". According to the International Y2K Center, of the ten participating South America countries, only Chile reported that they had sectors Y2K-ready before June 1999. Only Brazil shows evidence of awareness at the state/provincial level. On a regional level, the Organization of American States (OAS) has a working group on Y2K, which sponsors a South American forum on Y2K to assist countries who are late to the issue[16].

Many Central American countries are still struggling with the aftermath of Hurricane Mitch, which destroyed a great deal of critical infrastructure. In this context, Y2K remediation has been a lower priority. Awareness is generally high for banking and financial services as well as at major air transportation facilities. Nonetheless, Y2K does have the potential to push vulnerable sectors, such as drinking water, public services, and public health care, from bad to worse. Unfortunately, the lack of publicly available information for many countries in the region makes assessment difficult. In general, this region is characterized by low dependency on technology, but low Y2K progress.

Of note is the readiness of the Panama Canal, which reverts to Panamanian control on December 31, 1999. To avoid potential accidents, officials of the Panama Canal will require all ships to demonstrate Y2K compliance before entering the canal.

Mexico: Mexico economically dominates, and is believed to be among the best prepared countries in Latin America. According to Global 2000, Mexico received as good an overall rating, if not better, than the U.S.

Efforts in Mexico are led by the Year 2000 National Conversion Commission of Mexico, which includes representatives of private and public institutions. Strategic sector working groups are headed by specific industry leaders and/or public agencies. Overall assessments of Y2K readiness have been divided into finance, public sector, and private sector (non-financial). As of the May 1999 survey, the status of remediation is as follows:

Financial industry 99%
Government services 95%
Large companies 97%
Medium sized companies 80%
Small companies 53%

According to the August report, "*Upon comparison of the three surveys, it can be observed that, of the total of 145,000 establishments identified by the third survey as having out-of-date equipment connected to a network, there has been a nearly 100% increase in the level of awareness building and the involvement of top management, irrespective of the size of the establishments."*

Argentina: The International Y2K Center reports that all sectors will reach compliance between August and November 1999, with the financial sector leading the pack. The health sector lags, not expecting full implementation until November 1999. Of greatest concern, however, is the air transportation sector, which is highly dependent upon technology and is not expecting implementation until September 1999.

For the dozen largest gas utilities in Argentina, as of August 26, 1999, progress in implementing Y2K programs was 82%-92%.[17] The electric power industry is similarly advanced, with 82% of the generation, 86% of the transmission, and 78.5% of the distribution systems' Y2K implementation plans completed.[18]

Brazil: As the world's eighth largest economy, Brazil's exposure to Y2K risk could trigger economic problems outside of the region. Brazil is highly dependent upon telecommunications, electric power grids, air traffic control, banking and finance. Disruptions among Brazil's 4.5 million small- to medium-sized enterprises, which constitute over 50% of the labor force, could be severe given the lack of awareness and Y2K planning in these organizations.

Air Traffic Control: Brazil's national airline began its Y2K program in 1996, and the aircraft manufacturer Embraer has reportedly completed work on mission-critical systems. According to the International Aviation Transportation Association, $2.3 billion has been invested in remediating and modernizing air traffic control systems in Brazil.

Banks and finance: The Brazilian Federation of Bank Associations announced May 3, 1999 that a test conducted for more than 80% of the financial transactions was successful. The Central Bank of Brazil states that it will close unprepared banks and had set December 31, 1998 as the date for completing remediation of systems, a deadline

that Banco Cidade apparently made.

Telecommunications: Incomplete information about smaller providers is balanced by generally positive trends from industry-wide testing and leadership by major telecom firms. Industry-wide testing occurred July 31, 1999. The Gartner group expects limited and sporadic telephone outages in Brazil.

Electrical Power and Gas: The National Electric Power Agency had directed all 78 power distributors to be Y2K-ready by 30 June 1999. For gas, State-run Petrobas is stockpiling crude oil and refined products for year end shortages. According to Brazil's Y2K Coordinator, Marcos Osorio, the energy sector is running behind, but he expects only isolated problems[19].

Chile: According to Global 2000, Chile achieved readiness in the financial sector early in 1999, but several sectors require additional implementation or public information. As of August 16, 1999, Chile[20] is estimating 75% readiness across all sectors, up from 48% in December 1998. More specific findings are as follows:

- Banking 92%
- Electricity 68%
- Telecommunications 88%
- Transportation 76%
- Central Government 62%

The report notes that the readiness percentage is distinct from the probability of failure.

Chile expects to spend about $1.5 billion (including private sector), or roughly 2 percent of GDP. Air transportation was expected to be ready by the end of August 1999, and customs officials have been requiring Y2K compliant equipment since 1997.

Peru: According to Global 2000, as of June 15, 1999, Peru is, across many sectors, either not Y2K ready, or that public information is inadequate. Customs officials are expecting to finish remediation of systems by November 1, 1999, however, some glitches are expected. The public health system is vulnerable due to a lack of resources to replace or fix non-compliant medical equipment. The Gartner Group and the World Bank offer contradictory information, ranking Peru as one of the better prepared in South America.

Venezuela: Recent political problems have highlighted the inherent social and economic instability, and distracted efforts away from Y2K. Venezuela is a major oil exporter to the U.S., and oil exports account for 78% of Venezuela's export trade. Outside of the water transportation systems and ports, the major vulnerability for Venezuela is the electric power industry, which can be expected to experience some failures. Electricidad de Caracus (EDC), Venezuela's largest private utility, has invested $7 million on Y2K, but in general, Y2K readiness information from Venezuela is minimal.

Ecuador: 4 - 5% of the gross domestic product of Ecuador, or

about $143 million, is expected to be spent on Y2K fixes. Half of Ecuador's phone lines may not work unless contingency plans are put in place to deal with computer glitches, according to a spokesperson for government-owned Pacifitel. This situation has earned Ecuador a red on the Global 2000 chart for telecommunications. The energy sector also received a red for its lack of readiness or publicly available information, and no sector received a green "light". A study conducted in April 1999 by IBM of 54 Ecuadorian public institutions found that 45% have hardware problems and 40% have software problems.

Africa

The third conference of the Commission for Eastern African Co-operation, involving the heads of the Y2K programs of Kenya, Tanzania, and Uganda on September 7, 1999 identified critical cross-border issues requiring additional cooperation:

- Energy, notably electricity and petro-chemicals;
- Communications, especially telephones and data transmission;
- Finance, notably banks and other financial institutions; and,
- Transport, such as civil aviation and maritime services.

Uganda: Uganda has set up a National Y2K Task Force to assess the most critical socio-economic sectors of Uganda. A July position statement noted that more top management involvement in Y2K activities in various organizations and a general trend of accelerated progress.

That report highlighted the Red status of the Uganda National Examination Board in the government's critical computer services sector. The government is seriously concerned that at the rate the Board is progressing, it may not solve its problem in time to avoid serious disruptions to Uganda's educational cycle. Other sectors are yellow.

The status of the nation's most critical organizations is expected to be generally complete by September 9, 1999.

Rwanda: Rwanda's National Steering committee of 14 members from the public and private sectors was set up in January 1999. It operates under the auspices of the Ministry of Transportation and is chaired by the Minister. The most recent status shows:

Civil aviation: inventory and assessment showed the airport had the highest risks in the country, but negotiations were underway to install new equipment and systems.

Telecommunications: Y2K problems were observed in telex, communications equipment, and the billing system. Plans are to install new equipment and a new billing system, and to phase out telex.

Electricity: The highest risks are posed by the cash power billing system. Systems are being replaced.

Caisse Sociale: The risks are very high. By October they will have an upgraded compliant system.

Kenya: The Kenyan government established a National Year 2000 Steering Committee and a National Year 2000 Coordination Centre to coordinate national compliance efforts. The President has stated, "All of us are Y2K Stakeholders—Doing nothing is not an option."

Most essential public utilities were to be Y2K compliant by June. A March survey showed that commercial banks were 90% compliant, nonbank financial institutions were 92% compliant, and mortgage companies were 100% compliant.

EXPECTATIONS

The Committee is greatly concerned about the international Y2K picture. Several important U.S. trading partners are severely behind in addressing the Y2K problem. This leads the Committee to conclude that many short-term, and in some cases long-term, disruptions to supply chains are likely to occur.

If this proves to be true, such disruptions may cause a low-to-moderate downturn in the U.S. economy, particularly in industries that depend on foreign suppliers. However, the technology and business interconnections and interrelationships are difficult to map. This makes it impossible for the Committee or anyone else to predict which industries will be affected, and how much impact these affected industries will have on the economy.

In addition, there may be a request for humanitarian relief from developing countries that have not addressed the Y2K problem. The U.S. government should be establishing what are policy should be in responding to these requests should they arise.

CONCERNS

The Committee remains extremely concerned about the impact Y2K will have on the U.S. economy and our strategic interests. Several countries of strategic and economic importance to the U.S. are severely behind in their Y2K remediation efforts.

The regions of most concern to the Committee are Eastern Europe, Africa, and parts of Asia and South America. When considering strategic and economic factors, and the status of Y2K remediation efforts, the specific countries of most concern to the Committee are China, Russia, Italy, and several of the countries from which the U.S. imports oil.

[1] "The Year 2000 Problem and the Global Trading System," U.S. Department of Commerce, International Trade Administration, April 1999, p. 1, at http://y2k.ita.doc.gov/y2k.

[2] Id. at 12-13.

[3] "The 'Millennium Bug': The Preparedness of Key EU Infrastructures for the Y2000 Date Change," European Commission, COM(1999)275.

[4] See http://www.intl-monitoring.com/expatris.htm.

[5] See at www.abs.gov.au.

[6] See at http://www.comitatoanno2000.it/pres1.htm.

[7] See www.belgacom.be.

[8] See www.millennium.ch/

[9] " Y2K Bug Threatens Russian Computers" Alan S. Cullison,The Wall Street Journal July 13, 1999

[10] "The Russian Federation's Y2K Policy: Too Little, Too Late?" by W. McHenry and L. Malkov Communications of AIS Volume 2, Article 10 8 "The Russian Federation's Y2K Policy: Too Little, Too Late?"

[11] The first generation--the VVER-440 Model V230--operates at four plant sites in three countries: Russia, Bulgaria and the Slovak Republic. The second generation--the VVER-440 Model V213--operates at five plant sites in five countries: Russia, Ukraine, Hungary, the Czech Republic and the Slovak Republic. The third generation—the VVER 1000--operates at eight plant sites in three countries: Russia, Ukraine and Bulgaria.

[12] http://insp.pnl.gov:2080/?profiles/russia/#cprofile

[13] IBID

[14] See www.intl-monitoring.com/aseandan.htm

[15] See www.currents.net/newstoday

[16] http://www.oas.org/y2k/

[17] National Telecommunications Commission of Argentina, enargas.gov.ar

[18] (Argentine Electrical Industry) Compania Administradora del Mercado Mayorista Electrico SA – CAMMESA. Cammesa.com.ar

[19] "Bogota: Bermuda Insists", Associated Press, April 18, 1999.

[20] Inter-ministerial 2000 Action Committee of Chile (*Comite Interministerial Accion Chile 2000*), www.a2000.cl